



APR 3

Attorney Ref: 3282-C-2-Z  
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of:

Chang Lim et al

Art Unit 2155

Application No. 10/796,051

Examiner: Bharat Barot

Filed: March 10, 2004

For: INTERNET-ENABLED SERVICE MANAGEMENT SYSTEM AND METHOD

APPEAL BRIEF TRANSMITTAL

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Attached hereto are three (3) copies of the BRIEF ON APPEAL for the above-identified application. The fee in the amount of \$500.00 is submitted herewith.

Any additional fees necessary to effect the proper and timely filing of this Brief may be charged to Deposit Account No. 26-0090.

Respectfully submitted,

*Jim Zegeer*

Jim Zegeer, Reg. No. 18,957  
Attorney for Appellants

Attachments: Brief on Appeal (3 copies)

Suite 108  
801 North Pitt Street  
Alexandria, VA 22314  
Telephone: 703-684-8333

Date: April 3, 2006

In the event this paper is deemed not timely filed, the applicant hereby petitions for an appropriate extension of time. The fee for this extension may be charged to Deposit Account No. 26-0090 along with any other additional fees which may be required with respect to this paper.

Attorney Ref: 3282-C-2-Z  
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

re application of:

Chang Lim et al

Art Unit 2155

Application No. 10/796,051

Examiner: Bharat Barot

Filed: March 10, 2004

For: INTERNET-ENABLED SERVICE MANAGEMENT SYSTEM AND METHOD

**BRIEF ON APPEAL**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This is an appeal from the final rejection mailed October 3, 2005 finally rejecting Claims 7 - 14, 27 - 33, 39 and 40 of the above-identified application.

**(i). The Real Party in Interest**

The real party in interest is Alcatel Canada Inc..

**(ii). Related Appeals and Interferences**

There are no related appeals or interferences.

**(iii). Status of the Claims**

Claims 7 - 14, 27 - 33 and 39 and 40 are on appeal. All other claims have been cancelled.

**(iv). Status of the Amendments**

There was no amendment filed after the final action of October 3, 2005.

**(v). Summary of Claimed Subject Matter**

The invention is in the field of management of communication services from a service provider by a customer of the provider and gives the customers the ability to monitor and manage their outsourced network services, thus giving them control of their virtual private network (VPN).

The claimed subject matter may be divided into three main aspects or features:

1. system for authorizing the user of a client to have access to a server via the internet,
2. context sensitive help, and
3. multiple application using shared memory.

**First Aspect**

The first aspect is a system for Authorizing a user of a client to have access to a server via the internet. The problem solved by this aspect of the invention is as follows:

In the past, a user logs onto an internet application by providing a user identification (ID) and user password. The user remains logged onto the system until either the user logs out of the application or the user's session is timed out by the server

application. Due to the statelessness of the HTTP protocol, this mechanism does not allow multiple logon of identical user IDs. It presents a problem if the user's internet browser crashes and the user wishes to re-logon to the system; the user would have to wait until his previous session is timed out by the server application before he can re-logon to the application. This logon mechanism also disallows a user from switching to another workstation to logon to the application while having a current active session on another workstation; the user either needs to log out from the application from his original workstation or wait until his current session is timed out by the server application before the can logon from another workstation. The present invention solves this problem by providing a new logon authentication system which prevents multiple logon of the same logon ID and the ability to accommodate subsequent logon when a user's web browser has crashed or the user is operating from another workstation.

In addition, the logon authentication aspect of the invention prevents multiple logon of identical logon ID with the ability to accommodate subsequent logon when a user's web browser has crashed with the ability to logon from another workstation while having a current active session on another workstation. (See page 25 of the specification.)

As shown in Figs. 4 and 5 (reproduced below for convenience of reference), for each user, the application stores a user ID, the user password, status and an IP address.

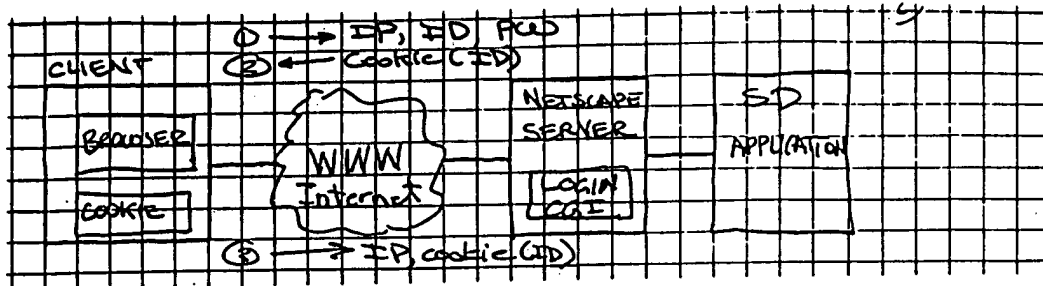


FIGURE 4

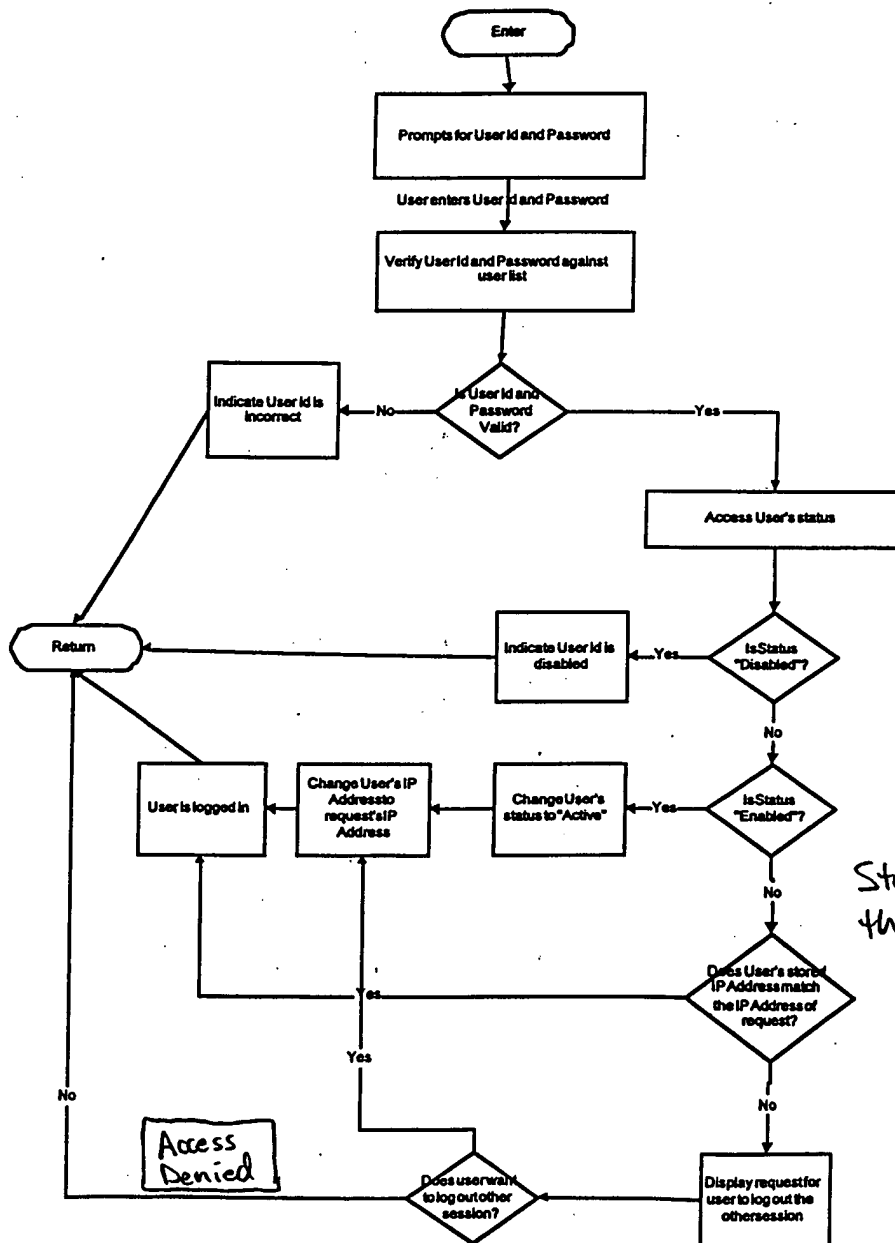


FIGURE 5

When the user requests access to a prescribed application, the application requires the user to enter his user ID and the user password. The application validates the information provided against the list of users stored in the application. If the user name and password match, the application checks the user's status in the application. If the user's status is "enabled" then the user is logged onto the system, and the user's status is changed to "active." The IP address of the user's workstation is retrieved by the server application; and the IP address is saved in the user's IP address field. If the user's status is "disabled", then the user is rejected. If the user's status is "active", then the application determines if the IP address of the current request matches with the stored user's IP address. If the IP addresses match, the user is logged onto the application. However, if the IP addresses to match (i.e. multiple logon of a user with the same user ID has been detected), a log out form will be displayed to inform the incoming user that a user with the same user ID is already in the system.

Thus, the client inputs user identification ID, the user password and the unique client address. The communication means at the client passes this information to the server via the internet in response to a request therefrom. The server stores the information respecting the client and compares the stored information with the user ID and password. The server stores dynamic status information respecting the user, the dynamic status

information being one of "enabled", "disabled" or "active" and the server includes being adapted to authorize access of the user if the ID and password agree with the stored information and the user status is "enabled".

### **Second Aspect**

The invention also features a system for providing context sensitive help information on a client's browser screen in response to a help request from a user. With reference to Figs. 7, 8 and 9 and specification pages 28, line 11 through page 33, line 22, the display screen includes a two-frame window on the browser screen (Fig. 8) including a content frame window (right) and a dashboard frame window (left). A help button associated with the dashboard frame window and a link is provided between a client and server whereby activation of the help button retrieves information relating to subject matter displayed on the content frame window from the server.

### **Third Aspect**

This aspect of the invention relates to the use of shared memory and is discussed at pages 39 - 41 of the specification. The invention provides network management in the context of network services. Hence there is a need to store extra information, such as user and customer profile. With the predefined nominal capacity of housing 500 customers and 1000 users, the cost of maintaining

another separate database is difficult to justify. The natural solution to this type of situation will usually be to store this additional information on disk file. However, the system has already have imposed a significant load on the system's performance; adding the file I/O bottle-neck is undesirable, especially in a concurrent system.

To optimize the performance, instead of storing the information onto the disk directly, the system writes the information into shared memory, and then updates the information to the disk periodically using a background control process. At the start-up of the system server, shared memory space is allocated and initialized by a daemon process. A handle to the shared memory is created and saved to a file. Server processes of user requests will look for that handle in order to access the shared memory. The structure and space requirement of the shared memory is also pre-defined. When a user's action requires access to the shared memory, the corresponding server process will use the structure definition as a map to access the shared memory space.

A separate background process is responsible for backing up the content of the shared memory. The process periodically updates the content to a backup file at a user-defined time interval. The backup file is used in system recovery and restart. The backup file is also updated right before system shutdown.

On the other hand, the daemon process creates a time-stamped backup of the shared memory at system startup time. It is done by



making a copy of the latest backup file and renaming it with a timestamp. The reason is to archive and preserve the configuration of the system before every startup. The shared memory is simply RAM that is used because access to a non-volatile storage device such as a hard drive is relatively slow. The fundamental idea is to read, in snapshot format from archive, into the shared memory and to write back again periodically.

A flow chart showing the backup procedure is given in Fig. 16.

In compliance with 37 CFR 41.37(c), there is attached hereto as Exhibit A a set of the claims on appeal wherein every means plus function and/or step plus function are identified and the structure material or acts described in the specification as corresponding to each of the claim function is set forth with reference to the specification by page and line numbers and to the drawings by reference characters where applicable.

**(vi). Grounds of Rejection to be Reviewed on Appeal**

1. The rejection of claims 7 - 12 and 39 - 40 under 35 U.S.C. 103(a) as being unpatentable over Baker et al (US 5,678,041) (hereinafter Baker) in view of Hu (US 5,586,260) (hereinafter Hu).
2. The rejection of claims 13 and 14 under 35 U.S.C. 103(a) as being unpatentable over LaStrange et al (US 5,784,058) (hereinafter LaStrange).
3. The rejection of claims 27 - 33 under 35 U.S.C. 103(a) as being unpatentable over Davis et al (US 5,796,952).

(vii). Argument

Ground 1.

First Feature or Aspect

The Examiner has erroneously rejected claims 7 - 12 and 39 - 40 under 35 U.S.C. 103(a) on the grounds that the subject matter would have been obvious with regard to the Baker patent in view of Hu.

Claim 7 is directed to a system for authorizing a user of a client to have access to a server via the internet wherein the client inputs information regarding the user ID and user password and client address. Communication means at the client passes the user ID, user password and client address to the server, via the internet, where it is stored along with dynamic status information with respect to the user with the dynamic status information being one of "enable", "disable" or "active". The user is authorized access only if the password agrees with the stored information and if said user status is "enabled".

No such arrangement and function is taught or suggested by the combination of Baker and Hu. Baker is directed to a system for restricting user access via the internet to certain rated information (the example used in the Baker patent is one of violent (V), nonviolent (NV) and/or moderately violent (MV)).

Independent claim 7 recites:

...communication means at said client for passing said ID, password and address to said server via said Internet in response to a request therefrom;....

No such communication means is found or shown in Baker: the proxy server 112 is at the user site 106. Figs. 1, 2 and 3 of Baker are reproduced in reduced form on the following page for convenience of reference:

FIG. 1

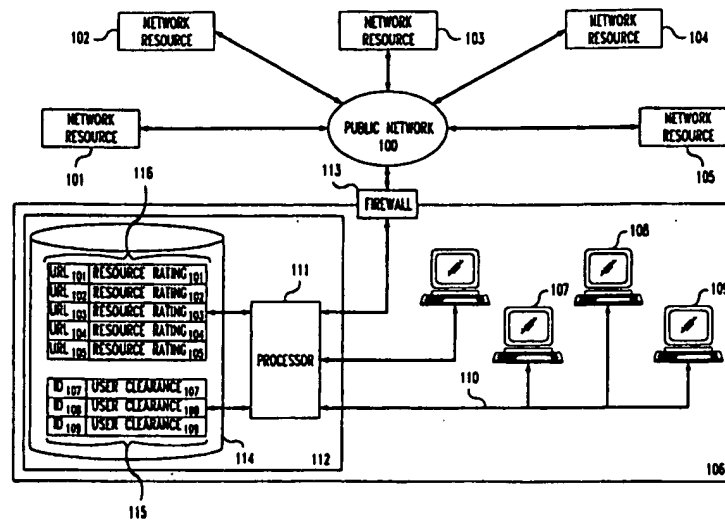


FIG. 2

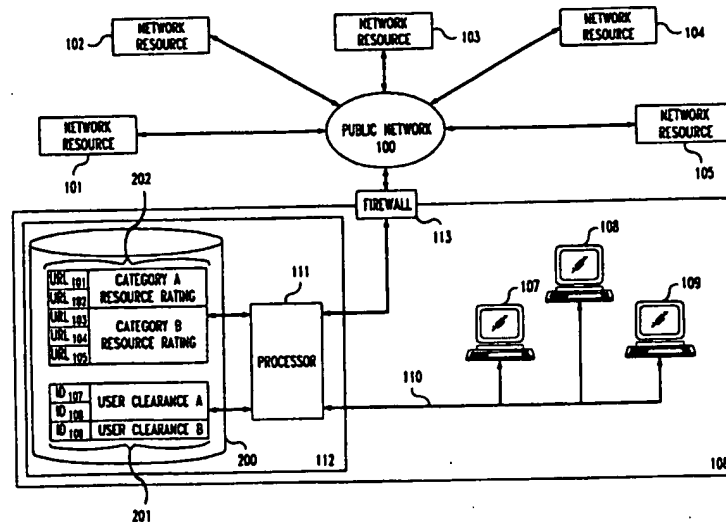
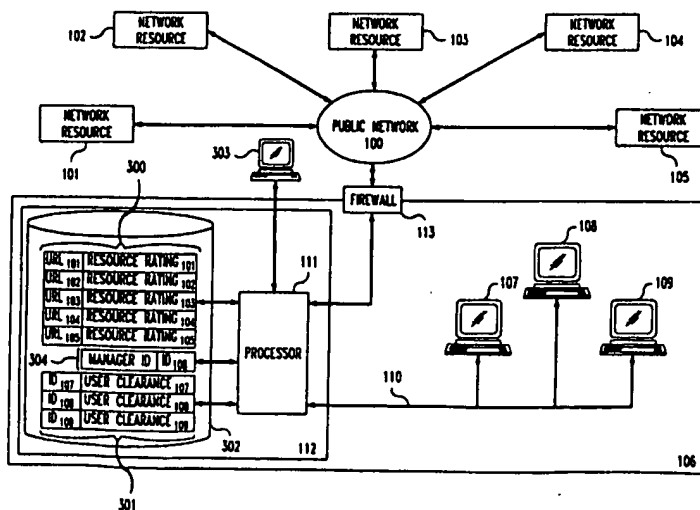


FIG. 3



Note that in each case the user sites 107, 108, 109 are coupled to the proxy server 112 and that the proxy server runs a check on the ID of each user to determine its level of clearance to receive a given resource which are rated and the rating stored in storages 114 (Fig. 1), 200 (Fig. 2) and 302 (Fig. 3). The user ID, user password, and client address are not transmitted through the public network or the internet 100 to the network resources 101, 102, 103, 104, 105 and 106. Hence, there is no communication means at said client for passing user ID, user password and client address to the network resources.

Furthermore, claim 7 recites:

...means at said server to store dynamic status information respecting said user, said dynamic status information being one of enabled, disabled or active;...

which finds no counterpart in the Baker reference.

The Examiner contends that, although Baker does not disclose a system having a means in the client for storing a unique client address and means at the client to store dynamic status information respecting the user, the status information being one of enabled, disabled or active, the Examiner contends that Hu makes up for this missing element in Baker. The Examiner refers to Fig. 4 in col. 1, lines 59 - col. 2, line 25 and col. 5, line 59 to col. 6, line 11 of Hu. Fig. 4 of Hu in the portions of the text cited by the Examiner are reproduced on the following page for convenience of reference:

FIG. 4 of Hu

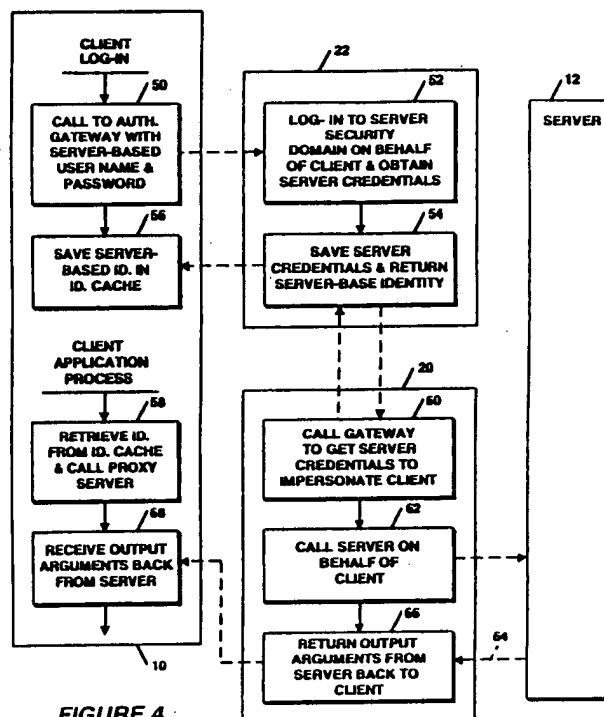


FIGURE 4

Pat. No. 5,586,260  
Col. 1, line 58 - Col. 2, line 25

More specifically, the step of mutually authenticating includes generating a set of security credentials that would enable the client to call the server; saving the security credentials for later use and generating an access key for their retrieval; and passing the access key to the client. Further, the step of calling the proxy server includes passing the access key to the proxy server; and the step of impersonating the client includes using the access key to retrieve the client security credentials needed to call the server.

In more specific terms, the method of the invention can be defined as comprising the steps of logging in to a server by calling, from the client system, an authentication gateway system, and supplying a user name and a security device; then obtaining, in the authentication gateway system, a set of security credentials that will permit client access to the server; and saving the security credentials and returning an access key to the credentials to the client. The next step is saving the access key in the client system. Subsequently, in a client application process, the client system performs the steps of retrieving the access key, calling a proxy server in the authentication gateway system, and passing the access key to the proxy server. Then, in the proxy server, the steps performed are using the access key to retrieve the security credentials, and using the retrieved security credentials to impersonate the client and call the server on the client's behalf. The step of logging in may include mutually authenticating the identities of the client and authentication gateway.

In addition, the method may include the steps of determining the identity of the client that logged in to the authentication gateway; determining the identity of the client that called and passed the access key; and comparing the client identities determined in the preceding two steps, to validate the identity of the client seeking access to the server.

Pat. No. 5,586,260  
Col. 5, line 58 - Col. 6, line 11

The steps performed in accordance with the method of the present invention are illustrated from a slightly different perspective in the flow chart of FIG. 4. In the client log-in process, a call is made to the authentication gateway process 22, as indicated in block 50. The log-in procedure prompts the user for a user name and a password based on the server security domain. In response to the call, the authentication gateway process 22 logs in to the server security domain on behalf of the client, as shown in block 52, and obtains the necessary server credentials, which are stored as a "security context" for the client, as indicated in block 54. Although not shown in block 52, the authentication gateway process 22 also invokes a service that provides the identity of the caller, i.e. the client, and stores the client identity with the security context information. As also shown in block 54, the authentication gateway process 22 returns a server-based identity to the client 10. The identity is basically an access key to retrieve the stored security context. In the client log-in process, the server-based identity is saved in a the id. cache, as indicated in block 56.

Note that Hu does not disclose any storing of status information which is one of enabled, disabled or active. Hu discloses storing "security credentials". These are different from status information. Moreover, Hu does not control the activity of the user station access by its status of enabled, disabled or active.

Baker, moreover, makes no mention of storing dynamic status information at all, being directed rather to a method of filtering site access requests based on ratings of content quality. In Baker and/or Hu, what happens if a second set of user ID, user password and client address is received at the server while the server is engaged with another user having the same user ID, user password and client address? Neither Baker or Hu give out any signal which is equivalent to enable, disable or active.

Method claim 12 is similar to apparatus claim 7, only cast in method format, and includes similar limitations of providing means at the server for recording dynamic status information respecting the user and the client, the status information being one of enabled, disabled or active, which is not found in the art.

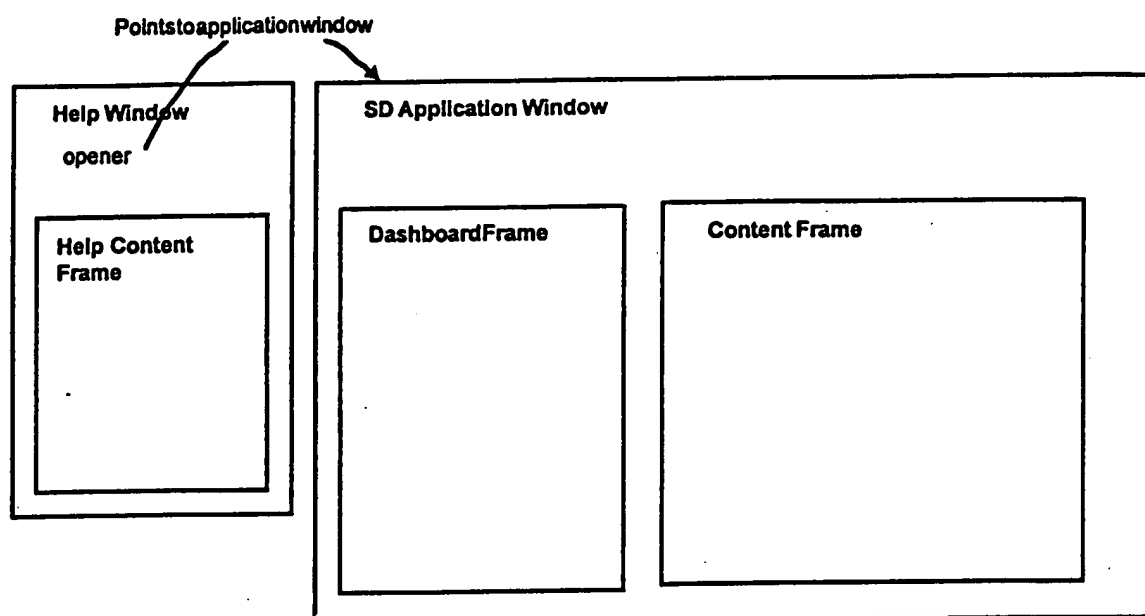
Claims 8 - 11, 39 and 40 are dependent on claim 7, and they are patentable for the reasons given above.

## Ground 2.

### Second Feature or Aspect

As to the second feature or aspect of the invention, the context sensitive help is defined in claims 13 and 14. The

Examiner's rejection of these two claims as being obvious under 35 U.S.C. 103(a) over LaStrange is clearly erroneous. These claims are directed to a system for providing context sensitive help information on a client's browser screen in response to help from a user. Fig. 8 is reproduced below for convenience of reference:



**FIGURE 8**

A two-frame window including a content window and a dashboard frame window are shown with a help button. Activation of the help button "retrieves help information relating to subject matter displayed on said content frame window from said server."

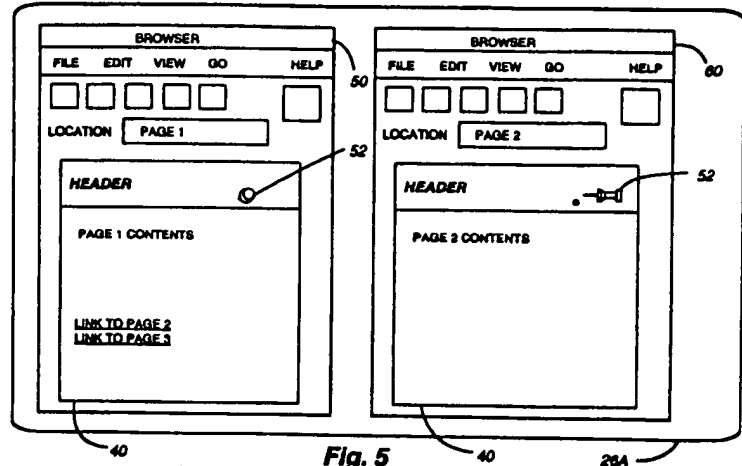
LaStrange fails to teach or suggest any "help" information system from a dual screen concept as taught by the present application and as recited in claims 13 and 14. The abstract and Fig. 5 of LaStrange are reproduced as follows:



Patent Number: 5,784,058

[57] ABSTRACT

The present invention provides a user control mechanism for selectively retaining for display a document obtained from a network. The user control is located as an icon or symbol in the browser interface for ease of use. Subsequent documents which are downloaded from the network are displayed in a separate window of the display in the computing system, and these subsequent windows are also provided with the same user control mechanism. In particular, the user can selectively create a second browser display page by following a link contained in the first browser display page, without overwriting the contents of the first browser display page.



LaStrange fails to teach or suggest any "help" information or any way to derive such help information from the dual screen concept, as taught by the present invention and as recited in claims 13 and 14. According to the abstract of LaStrange (reproduced above), LaStrange provides a user control mechanism for selectively retaining for display a document obtained from a network. The user control is located as an icon or symbol in the browser interface for each of use. Subsequent documents which are downloaded from the network are displayed in a separate window of the display in the computing system. In particular, the user can

selectively create a second browser display page by following a link contained in the first browser display page, without overwriting the contents of the first browser display page. (See Fig. 5 of LaStrange.) LaStrange opens a new browser window when a link is clicked, rather than replacing the contents of the existing browser window with new downloaded content. LaStrange makes no mention of a content frame window and a dashboard frame window, a help button associated with the dashboard frame window, or retrieval of help information relating to the contents of the content frame window for display on the frame window. The appellants respectfully submit that LaStrange does not teach or suggest every element and function of claims 13 and 14.

Appellants respectfully submit that the Examiner has erred in rejecting claims 13 and 14 as being obvious in view of LaStrange.

### Ground 3.

#### Third Feature or Aspect

Claims 27 - 33 are directed to a system for storing information respecting a plurality of applications to a shared memory. This feature of the invention comprises a volatile memory for storing the information and means to allocate space in the volatile memory to selected ones of the plurality of applications. An identification means for identifying the space to be allocated to each of the selected applications and a backup means to periodically transfer stored information from a volatile memory to

a non-volatile memory and means to retrieve the information from a non-volatile memory system start-up.

No such teaching or suggestion or such a teaching is disclosed or found in Davis.

The Examiner contends that:

... Davis does not explicitly disclose that retrieves [sic] the information from the non-volatile memory at system startup and stores the information to the non-volatile memory at system shutdown. But it would have been obvious and known in the art at the time the invention was made to retrieve the information from the non-volatile memory at system startup and store the information to the non-volatile memory at system shutdown because doing so would reduce data or information loss problem.

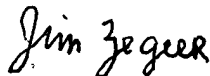
The Examiner has not cited a reference or evidence which would have rendered the element obvious. Furthermore, the Examiner alleges that Davis teaches the remaining elements of claim 27. Davis does not appear to teach backup means to periodically transfer stored information from the volatile memory to a non-volatile memory. Davis does not even appear to teach a system for storing information respecting a plurality of applications to a shared memory. In fact, Davis is directed to a method by which a tracking program is run on a client in order to track user browsing behavior, and this browsing behavior is transmitted to a server. Davis does not teach or suggest the invention defined in claim 27. Claims 28 - 33 are dependent on claim 27, include the same limitations, and are patentable for the same reasons. Finding the elements recited in a claim is one thing -- finding them in appellants' arrangement and functioning as claimed is something

altogether different. Appellants therefore submit that the Examiner committed error in rejecting claims 27 - 33 on the ground of being obvious in view of the Davis patent.

**CONCLUSION**

Appellants respectfully submit that the Examiner has erred in rejecting claims 7 - 14, 27 - 33, 39 and 40 and should be reversed.

Respectfully submitted,



Jim Zegeer, Reg. No. 18,957  
Attorney for Appellants

Attachment: CLAIMS APPENDIX  
EVIDENCE APPENDIX  
Exhibit A

Suite 108  
801 North Pitt Street  
Alexandria, VA 22314  
Telephone: 703-684-8333

Date: April 3, 2006

In the event this paper is deemed not timely filed, the applicant hereby petitions for an appropriate extension of time. The fee for this extension may be charged to Deposit Account No. 26-0090 along with any other additional fees which may be required with respect to this paper.

(viii) CLAIMS APPENDIX

7. A system for authorizing a user of a client to have access to a server via the Internet comprising:

means in said client for inputting a user identification (ID) and user password;

means in said client for storing a unique client address;

communication means at said client for passing said ID, password and address to said server via said Internet in response to a request therefrom;

means at said server to store information respecting said client and to compare said stored information with said user ID and user password;

means at said server to store dynamic status information respecting said user, said dynamic status information being one of enabled, disabled or active; and

means to authorize log in of said user if said ID and password agree with said stored information and if said user status is enabled.

8. A system as defined in claim 7 wherein said status information is changed to active when said user is granted access to said server.

9. A system as defined in claim 7 wherein said user is denied access to said server if said status information is disabled.

10. A system as defined in claim 7 wherein if said status information is active said server compares said client address with said stored information and if said address agrees with said stored information said user is logged onto said server, otherwise said user is denied access.

11. A system as defined in claim 7 wherein said client is an end user of an Internet-based customer service management system and said server is a service director having means to manipulate a user's virtual private network in a multi-technology network.

12. A method of controlling a client user's access to an Internet based server, comprising:

- providing means at said client for said user to input a user identification and a user password;

- providing means at said client for storing a client address;

- providing means at said client for passing said user identification, said user password and said client address to said server via said Internet when such information is requested by said server;

- providing means at said server for storing said user identification, said user password and said client address;

- providing means at said server for recording dynamically, status information respecting said user and said client, said status information being one of enabled, disabled or active;

- providing means at said server to compare said stored user identification, said user password and said client address with information input passed to said server from said client;

- and providing means at said server to allow said user to login to said server if said user identification and said user password agree with said stored information and said status information is active.

13. A system for providing context sensitive help information on a client's browser screen in response to a help request from a user comprising:

- a two frame window on said browser screen including a content frame window and a dashboard frame window;

- a help button associated with said dashboard frame window; and

link means between said client and a server,  
whereby activation of said help button retrieves help information  
relating to subject matter displayed on said content frame window  
from said server.

14. A system as defined as defined in claim 13 wherein said  
server is a customer services management (CSM) services director  
(SD) in a multi-technology digital network.

27. A system for storing information respecting a plurality  
of applications to a shared memory comprising:

a volatile memory for storing said information;  
means to allocate space in said volatile memory to selected  
ones of said plurality of applications;  
identification means for identifying said space allocated to  
each of said selected applications;  
backup means to periodically transfer stored information from  
said volatile memory to non-volatile memory; and  
means to retrieve information from said non-volatile memory at  
system startup.

28. A system as defined in claim 27 wherein said volatile  
memory is a random access memory (RAM).

29. A system as defined in claim 27 wherein said non-volatile  
memory is a hard disk storing device.

30. A system as defined in claim 29 wherein said means to  
allocate space is a daemon process.

31. A system as defined in claim 27 wherein said backup means  
stores said information to said non-volatile memory at system shut  
down.

32. A system as defined in claim 31 wherein said shared memory is in a server in an Internet based communication system.

33. A system as defined in claim 32 wherein said communication system is a customer service management system (CSM) and said server is a CSM service director.

39. The system as defined in claim 7 wherein said means to authorize log in includes means to prevent log in if said user is already logged in.

40. The system as defined in claim 7 wherein said status information relates to whether said user is enabled, disabled or active.



(ix). EVIDENCE APPENDIX

See attached Exhibit A.

Claims 7 to 12, 39, and 40

The subject matter of these claims is described from pages 25, line 1 to page 28, line 5 and Figs. 4 and 5.

Claim 7

- a) means in the client for inputting a user identification and user password

page 26, line 5: "When a user requests access to the SD application, the application requires the user to enter a user Id and a user password"

- b) means in the client for storing a unique client address

page 18 line 11: "User Ids and IP address are transferred within HTTP protocol request and response header for each request and response"

- c) communication means at the client for passing the ID password and client address to the server

page 27, line 19: "The client sends a TCP/IP message containing user Id and password to the server"

page 26, line 13: "The IP address of the user's workstation is retrieved through the environment variable "REMOTE\_ADDR" by the server application"

page 27, line 20: "The IP address of the client is included in the TCP/IP message"

- d) means at the server to store information respecting the client

page 26, line 3: "For each user the application stores a user Id, a user password, ...and an IP address"

- e) means at the server to compare the stored information with the user ID and user password

page 26, line 7: "The application validates the information provided against the list of users stored in the application"

- f) means at the server to store dynamic status information

page 26, line 3: "For each user the application stores ... a status"

page 26, line 12: "and the user's status is changed to active" (dynamic aspect)

- g) means to authorize log in of the user

page 26, line 9: "If the user name and password matches, the application checks the user's status in the application. If the user's status is "enabled" then the user is logged on the system"

#### Claim 11

- a) means to manipulate a user's virtual private network

page 5, line 9: "A network management system allows an operator to configure the network [including a user's VPN]"

#### Claim 12

- a) means at the client for the user to input a user identification and user password

same as (a) of claim 7

- b) means at the client for storing a client address

same as (b) of claim 7

- c) means at the client for passing the ID and password to the server

same as (c) of claim 7

- d) means at the client for passing the address to the server

same as (d) of claim 7

- e) means at the server for storing the user ID, password, and address

same as (e) of claim 7

- f) means at the server for recording dynamically status information

same as (g) of claim 7

- g) means at the server to compare stored information to information passed from the client

same as (f) of claim 7

- h) means at the server to allow the user to login to the server  
same as (h) of claim 7

#### Claim 39

- a) means to prevent log in if the user is already logged in  
  
page 27, line 6: "The third function [defined using Netscape Server API] services the logout form. For example, when a user tries to log into the system with a user Id which belongs to someone who has already logged onto the system ... a log out form will be displayed to inform the incoming user that a user with the same user Id is already in the system, and prompt him to log off the other session"

#### Claims 13 and 14

The subject matter of these claims is described from page 28 line 7 to page 33 line 23 and Figs. 7, 8 and 9.

#### Claim 13

- a) link means between the client and a server

A link between the client and the server is described early on in the description (see Fig. 1, Fig. 2, Fig. 3, Fig. 4), and is present since much of the description talks about transfer of HTML files (see for example pages 29 and 30) and use of HTTP. Also see page 28 line 12: "a user using an Internet based application" when introducing the need for an improved context sensitive help for users of Internet based applications.

#### Claims 27 to 33

The subject matter of these claims is described from page 39, line 18 to page 41, line 5 and in Fig. 16.

#### Claim 27

- a) means to allocate space in volatile memory to selected ones of the applications

page 40, line 8: "At the start up of the Service Directory server, shared memory space is allocated and initialized by a daemon process"

page 40, line 33: "The shared memory is simply RAM"

- b) identification means for identifying the space allocated to each application

page 40, line 14: "When a user's action requires access to the shared memory, the corresponding server process will use the structure definition as a map to access the shared memory space"

- c) backup means to periodically transfer stored information to non-volatile memory

page 40, line 19: "A separate background process is responsible for backing up the content of shared memory. The process periodically updates the content to a backup file"

- d) means to retrieve information from non-volatile memory at system startup

page 40, line 22: "The backup file is used in system recovery and restart"

FIG. 16: "Read in latest time-stamped backup from archive into shared memory"

**(x). RELATED PROCEEDINGS APPENDIX**

There are no proceedings as mentioned in section (i) above,  
and accordingly no decisions rendered.